Background on Protecting Information Privacy and Other Legal Rights in the context of the ISE

INTRODUCTION

Section 1016(d)(2)(A) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, December 17, 2004, (IRTPA) required the President to issue guidelines that "protect privacy and civil liberties in the development and use of the ISE." The President included the IRTPA mandate in Section 1 of Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (October 25, 2005), wherein he provided that, "[t]o the maximum extent consistent with applicable law, agencies shall … give the highest priority to … the interchange of terrorism information among agencies… [and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities …" In order to implement the requirements of IRTPA and various Executive Orders, the President, in Guideline 5 of his Presidential Memorandum of December 16, 2005, directed the Attorney General and the Director of National Intelligence to develop "…guidelines designed to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including the acquisition, access, use, and storage of personally identifiable information." The resulting *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (ISE Privacy Guidelines) were approved by the President and issued by the Program Manager for the ISE (PM-ISE) on December 4, 2006.

Section 2(a) of the ISE Privacy Guidelines specifically requires that "All agencies shall, without exception, comply with the Constitution and all applicable laws and Executive orders relating to protected information in the ISE." In Section 1(b) of the Guidelines, "Protected Information" is defined as "information about American citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and federal laws of the United States." These "other legal protections" derive primarily from the civil liberties guaranteed by the Constitution of the United States and the civil rights laws of the United States. Section 1(b) also states that Protected Information includes (for the intelligence community) "information about 'United States persons' as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive order, international agreement, or other similar instrument, should be covered by these guidelines."

WHAT IS INFORMATION PRIVACY?

The roots of the right to privacy in America are generally traced to an 1890 article by Samuel D. Warren and Louis D. Brandeis in the Harvard Law Journal. In "The Right to Privacy,"[1] the authors advocated "the right to be let alone" to counter the activities of

[1] http://www-swiss.ai.mit.edu/6805/articles/privacy/Privacy_brand_warr2.html

yellow journalists who were, according to the authors, turning gossip into an American industry. Warren and Brandeis believed that a right to be let alone existed in the common law, independent of any statutory protections.

Although many people associate "privacy" with the matters they would prefer to keep "private," the protections envisioned within the concept of privacy have grown beyond the notion that information about an individual should remain personal. Since the Warren and Brandeis article, privacy has become a multi-dimensional concept in the United States legal system, expanded to cover both substantive and procedural rights derived from constitutional, statutory, and common law sources. These disparate privacy rights range from the right to make decisions regarding family matters to the notice required before the Federal government obtains information from an individual. "Privacy" now refers to a number of context-specific legal protections.

With respect to the ISE, the focus is on "information privacy," a subset of the privacy protections derived from various sources of U.S. law. Information privacy generally relates to the ability to control information about oneself. The Privacy Act of 1974 protects the information privacy of U. S. citizens and lawful permanent residents (LPRs), imposing obligations on Federal agencies that collect and administer information about individuals, and affording individuals certain rights with respect to personal information these agencies collect. The Privacy Act embraces a set of "Fair Information Practices,"[2] embedded in its provisions, including:

(1) Notice: The Privacy Act requires agencies to post public notices explaining the manner in which personal information contained in a system of records is collected, used, protected, shared, and disposed.

(2) Right of Access and Correction: The Privacy Act generally affords individuals the right to view information Federal agencies collect about them and to request correction of information they believe is not accurate, relevant, timely, or complete.

(3) Collection Limitations: The Privacy Act places limits on the personal information that an agency may collect by requiring that it be relevant to authorized agency purposes and that, to the extent possible, collected directly from the individual who is the subject of the information.

(4) Data Quality: The Privacy Act requires Federal agencies to maintain records with the degree of accuracy, relevance, timeliness, and completeness as is necessary for their intended use.

---

[2] Although these rights have come to be known as the "Fair Information Practices," they are not labeled as such in the Privacy Act.

(5) Consent to sharing: The Privacy Act requires that agencies share information about individuals only with the consent of the individual or, absent consent, only as specifically provided by the statute.

(6) Security: The Privacy Act requires Federal agencies to implement administrative, technical, and physical controls as needed to protect information collected and maintained in agency systems against loss, unauthorized access, disclosure, modification, use, or destruction.

(7) Accountability: The Privacy Act prescribes civil amd criminal penalties that may be imposed on Federal agencies and employees of Federal agencies for failing to comply with the statute's requirements.

WHAT ARE CIVIL RIGHTS AND CIVIL LIBERTIES?

The term *civil liberties* is much broader than the concept of privacy and, in fact, embraces privacy, despite the fact that these are sometimes viewed as mutually exclusive legal protections.[3] Although there is no universally accepted definition of *civil liberties*, the Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) defines the term as follows:

> The term *civil liberties* refers to fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments—to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference in relation to the specific freedoms enumerated in the Bill of Rights."[4]

No civil liberties are absolute. Their exercise must be weighed against other factors (e. g., security and the safety of others). The basic civil liberties include:

- **Freedom of association:** the right to choose people with whom to associate.
- **Freedom of assembly:** the right to gather in groups, clubs, or organizations, including any political party, special interest group, or union.

---

[3] In Griswold v. Connecticut, 381 U.S. 479, 85 S. Ct. 1678, 14 L. Ed. 2d 510 (1965), the U.S. Supreme Court found that the specific guarantees in the Bill of Rights have penumbras "formed by emanations from those guarantees that help give them life and substance" and the right to privacy exists within this penumbra. This penumbra doctrine essentially means that there are certain implied powers that emanate from specific constitutional provisions.

[4] National Criminal Intelligence Sharing Plan (NCISP), p. 5, available at http://www.iir.com/global/products/NCISP_Plan.pdf. See also, *DOJ's Global Justice Information Sharing Initiative, Privacy, Civil Rights and Civil Liberties: Policy Templates for Justice Information Systems*, September, 2006, at 3 (adopting the NCISP definition) http://www.it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf

- **Freedom of religion:** the right to choose the religion in which to believe and to worship in the manner of one's choosing, including the freedom not to follow any religion.
- **Freedom of speech:** the right to speak freely without censorship.
- **Due process of law:** the protection against government action to deprive one of life, liberty, or property without following established procedure.
- **Right to a fair trial:** the right of criminal defendants to a speedy trial, an impartial judge and jury, assistance of counsel and, the opportunity to confront one's accuser.

The term "civil rights" is much narrower in scope. Global defines the term as follows:

> The term *civil rights* is used to imply that the state has a role in ensuring all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress. Generally, the term *civil rights* involves positive (or affirmative) government action, while the term *civil liberties* involves restrictions on government."[5]

Depending on an agency's mission and the ramifications to protected individuals of sharing information in the ISE, a variety of civil rights laws may be implicated, potentially including:

- The Civil Rights Act of 1964, as amended, 42 U.S.C. §2000e, *et seq*.
  - Title I (barring unequal application of voter registration requirements);
  - Title II (prohibiting discrimination in public accommodations);
  - Title III (prohibiting discriminatory denial of access to public facilities);
  - Title VI (preventing discrimination in federally funded programs);
  - Title VII (prohibiting discrimination in employment).
- The Rehabilitation Act of 1973, Pub. L. 93-112, 29 U.S.C. §701 *et seq*.
  - Section 794 (rights, advocacy, and protections for individuals with disabilities);
  - Section 504 (prohibiting discrimination based on disability in programs or activities receiving Federal funds).
- The Equal Educational Opportunities Act of 1974, 20 U.S.C. §1701 *et seq*. (prohibiting discrimination in educational opportunities based on race, color, sex, or national origin).
- The Americans with Disabilities Act, 42 U.S.C. §12101 *et seq*.
  - Title I (prohibiting employment discrimination against a qualified individual with a disability);

[5] Id at 5-6. See also the modified definition of *civil rights* in the Key Issues Guidance Paper, "Civil Rights and Civil Liberties Protection Guidance."

    - Title II (prohibiting denial of services and benefits by reason of disability);
    - Title III (prohibiting discrimination on the basis of disability in public accommodations (e.g. schools) operated by private entities.
- The Fair Housing Act, 42 U.S.C. §3601 (prohibiting housing discrimination based on race, color, religion, sex, national origin, familial status, or disability).
- The Voting Rights Act of 1965, 42 U.S.C. §§1973 - 1973aa-6 (protecting Americans against racial discrimination in voting).
- The Civil Rights of Institutionalized Persons Act, 42 U.S.C. §1997 *et seq*. (protecting the rights of inmates to medical/mental health care, fire safety, sanitation, access to courts, and protection from abuse by staff and inmates).

HOW DO THE ISE PRIVACY GUIDELINES PROTECT PRIVACY AND CIVIL LIBERTIES?

The ISE Privacy Guidelines establish a framework for sharing information in the ISE in a manner that protects privacy and civil liberties. The framework balances the dual imperatives of information sharing and protecting privacy by establishing uniform procedures to implement existing protections, or develop additional safeguards, in unique legal and mission environments. The Guidelines build on a set of core principles that require specific, uniform action across Federal agencies and departments and reflect long-standing privacy protections and best practices. The Guidelines do not and cannot override existing laws, such as the Privacy Act. Instead, the ISE Privacy Guidelines require agencies to assess, document, and enforce the rules applicable to the protected information that they seek to access or make available via the ISE and to take uniform steps to ensure that essential privacy and civil liberties principles are honored as they develop and use the ISE.

The ISE Privacy Guidelines require each agency to develop a written ISE privacy protection policy addressing: identification of data eligible to be shared; notice of the nature of the data shared (e.g., whether it pertains to U.S. citizens, lawful permanent residents, or other protected persons); assessment of the legal and policy restrictions applicable to the data and implementation of necessary additional safeguards; mechanisms for accountability, enforcement, and audit; measures to ensure data quality and data security; and coordination of internal and external redress procedures. Each agency's designated ISE Privacy Official will ensure compliance with the Guidelines. In sum, as agencies determine what information they can make available to others and what information they will access in the ISE, they will assess the applicable privacy and civil liberties protection framework, and institute safeguards specific to the type of information and sharing involved.

Non-Federal entities seeking to access protected information through the ISE, including State, local, and tribal governments and private agencies, must develop and implement policies and procedures that provide protections at least as comprehensive as those contained in the ISE Privacy Guidelines.